IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A system for providing dynamic screening of transient messages in a distributed computing environment, comprising:

an antivirus system intercepting an incoming message at a network domain boundary, the incoming message including a header comprising a plurality of address fields storing contents;

a stored set of blocking rules, each blocking rule defining readily-discoverable characteristics indicative of messages infected with at least one of a computer virus, malware and bad content;

a parser module identifying the contents of each address field;

a comparison module checking the contents of each address field against the blocking rules to screen infected messages and identify clean messages;

an intermediate message queue staging each such clean message pending further processing;

an antivirus scanner scanning each message in the intermediate message queue for at least one of a computer virus and malware; and

an event handler performing each scanning operation as an event responsive to each such clean message staged in the intermediate message queue;

wherein the infected messages are blocked from entering the intermediate message queue immediately after the comparison is made between the blocking rules and the contents of at least one of the address fields;

wherein the intermediate message queue is maintained at a constant size;

wherein the constant size is determined according to a progress of the antivirus scanner in order to prevent the intermediate message queue from becoming overloaded with messages awaiting scanning.

2. (Original) A system according to Claim 1, further comprising: